IEEE 802.11i-2004

From Wikipedia, the free encyclopedia
(Redirected from 802.11i)

IEEE 802.11i-2004 or **802.11i** is an amendment to the original IEEE 802.11 standard specifying security mechanisms for wireless networks. It replaced the short *Authentication and privacy* clause of the original standard with a detailed *Security* clause, in the process deprecating the broken WEP. The amendment was later incorporated into the published IEEE 802.11-2007 standard.

Contents

- 1 Description
- 2 Encryption key distribution
  - 2.1 The Four-Way Handshake
  - 2.2 The Group Key Handshake
- 3 See also
- 4 References

Description

The draft standard was ratified on 24 June 2004, and supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as **WPA2**, also called **RSN** (Robust Security Network). 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher.[1]

The 802.11i architecture contains the following components: 802.1X for authentication (entailing the use of EAP and an authentication server), RSN for keeping track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication. Another important element of the authentication process is the four-way handshake, explained below.

Encryption key distribution

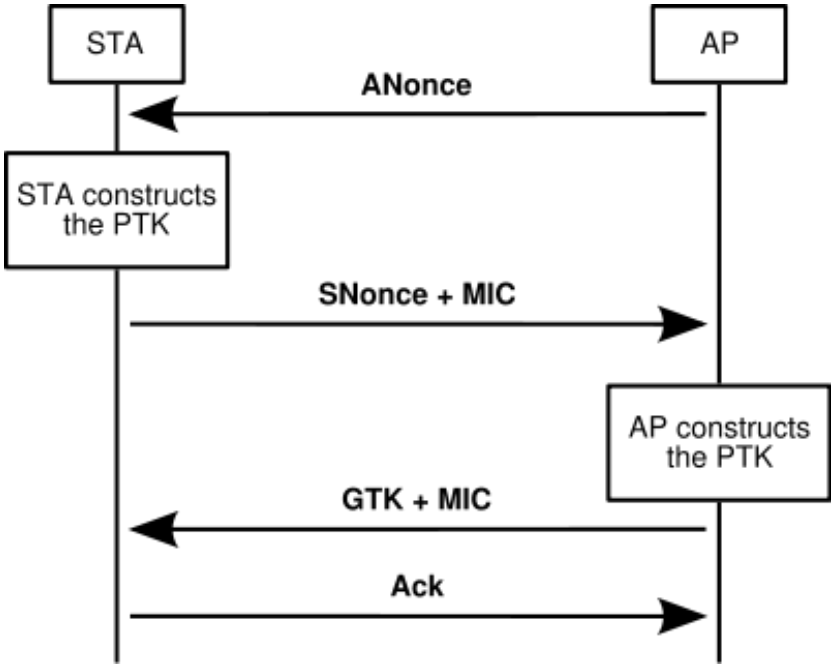
The IEEE 802.11i-2004 introduced new key distribution methods to overcome weaknesses in earlier methods. This method works with any RSNA network, whether WPA or WPA2, TKIP or CCMP (AES).

The Four-Way Handshake

The authentication process leaves two considerations: the access point (AP) still needs to authenticate itself to the client station (STA), and keys to encrypt the traffic need to be derived. The earlier EAP exchange has provided the shared secret key PMK (Pairwise Master Key). This key is however designed to last the

entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish another key called the PTK (Pairwise Transient Key). The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address and STA MAC address. The product is then put through a cryptographic hash function.

The handshake also yields the GTK (Group Temporal Key), used to decrypt multicast and broadcast traffic. The actual messages exchanged during the handshake are depicted in the figure and explained below:



1. The AP sends a nonce-value to the STA (ANonce). The client now has all the attributes to construct the PTK.
2. The STA sends its own nonce-value (SNonce) to the AP together with a MIC, including authentication, what really is a Message Authentication and Integrity Code: (MAIC).
3. The AP sends the GTK and a sequence number together with another MIC. The sequence number is the sequence number that will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The STA sends a confirmation to the AP.

All the above messages are sent as EAPOL-Key frames.

As soon as the PTK is obtained it is divided into five separate keys:

PTK (Pairwise Transient Key – 64 bytes)

1. 16 bytes of EAPOL-Key Encryption Key (KEK) - AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client (for example, the RSN IE or the GTK)
2. 16 bytes of EAPOL-Key Confirmation Key (KCK)– Used to compute MIC on WPA EAPOL Key message
3. 16 bytes of Temporal Key (TK) – Used to encrypt/decrypt Unicast data packets
4. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on unicast data packets transmitted by the AP
5. 8 bytes of Michael MIC Authenticator Rx Key – Used to compute MIC on unicast data packets transmitted by the station

The Michael MIC Authenticator Tx/Rx Keys provided in the handshake are only used if the network is

using TKIP to encrypt the data.

The Group Key Handshake

The GTK used in the network may need to be updated due to the expiry of a preset timer. When a device leaves the network, the GTK also needs to be updated. This is to prevent the device from receiving any more multicast or broadcast messages from the AP.

To handle the updating, 802.11i defines a *Group Key Handshake* that consists of a two-way handshake:

1. The AP sends the new GTK to each STA in the network. The GTK is encrypted using the KEK assigned to that STA, and protects the data from tampering, by use of a MIC.
2. The STA acknowledges the new GTK and replies to the AP.

GTK (Groupwise Transient Key – 32 bytes)

1. 16 bytes of Group Temporal Encryption Key – Used to encrypt Multicast data packets
2. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on Multicast packet transmitted by AP
3. 8 bytes of Michael MIC Authenticator Rx Key – This is currently not used as stations do not send multicast traffic

The Michael MIC Authenticator Tx/Rx Keys provided in the handshake are only used if the network is using TKIP to encrypt the data.

See also

- WLAN Authentication and Privacy Infrastructure (WAPI), China's centralized wireless security method
- Wi-Fi Protected Setup

References

- "IEEE 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications". IEEE. 2007-03-08. http://standards.ieee.org/getieee802/802.11.html.

1. ^ "IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements" (pdf). IEEE Standards. 2004-07-23. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf. Retrieved on 2007-12-21.